UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,476	12/17/2003	Marilyn S. Bullock	014033-000006	1475

24239 7590 10/06/2008

MOORE & VAN ALLEN PLLC
P.O. BOX 13706
Research Triangle Park, NC 27709

EXAMINER	
MURDOUGH, JOSHUA A	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
10/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/707,476	BULLOCK ET AL.	
	Examiner	Art Unit	
	JOSHUA MURDOUGH	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 C.F.R. §1.114

1. A request for continued examination (RCE) under 37 C.F.R. §1.114, including the fee set forth in 37 C.F.R. §1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 C.F.R. §1.114, and the fee set forth in 37 C.F.R. §1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 C.F.R. §1.114. Applicant's submission filed on 29 July 2008 has been entered.

Acknowledgements

2. As noted above, this action is responsive to the RCE filed on 22 September 2008 requesting that the after final response dated 29 July 2008 be entered.

3. Claims 1-36 are pending and have been examined.

4. The Examiner has referenced three press releases regarding the same product. These press releases (From Panda Security Internacional; dated Jan. 17, 2001; Nov. 15, 2001; and Nov. 26, 2002) all reference a single embodiment ("Panda ActiveScan" 4.0), but when cited, the Examiner has referred to them chronologically as "Release 1," "Release 2," and "Release 3." See MPEP 2131.01.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 4, 10, 11, 13, 14, 16, 22, 23, and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hoene (US 2002/ 0199116) in view of Antur (US 6,212,558).

7. As to claims 1, 13, and 22, Hoene shows:

a. A method of disabling malicious code residing on a customer computer system (Step 178, Figure 3) through a network (Figure 1), the method comprising:

b. authenticating the customer (client 20) for the on-line services (Step 152, Figure 3);

c. presenting to the customer an option to perform a scan of the customer computer system for the malicious code (client either runs the virus scan or does not connect, Step 162, Figure 3);

d. executing, at least in part by activation over the network (Step 158, Figure 3) and upon receiving from the customer a selection of the option to perform the scan (Step 154, Figure 3), computer program instructions for performing the scan (McAfee, [0018]), the computer program instructions being directed to detection and disablement of the malicious code (Step 206, Figure 4) so that network extends its security perimeter around the customer (the client becomes part of the network by connecting to the server, Figure 1; therefore, the client is considered safe while connected and the virus scan remains active, Steps 180 and 184, Figure 3) while the customer is performing on-line transactions (Step 204, Figure 4);

8. Hoene does not expressly teach:

e. association with a financial institution providing on-line financial services to a customer; and

f. providing the on-line financial services to the customer.

9. However, Antur teaches a secure network (C 1, LL 11-17) with a security perimeter (C 5, LL 47-55) intended for use in financial services from a financial institution (financial services companies, C 1, LL30-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the teachings of Hoene to apply the virus scanning and other control aspects to the financial services network as shown by Antur instead of the generic network disclosed, in order to counter the risks of endangering information assets (Antur, C 1, LL30-40).

10. As to claims 2, 14, and 23, Hoene further shows:

the executing of the computer program instructions further comprises downloading the computer program instructions to the customer computer system (network provided software, [0023]).

11. As to claims 4, 16, and 25, Hoene further shows:

the computer program instructions are operable to perform signature-based detection of the malicious code (Step 158, Figure 3).

12. As to claim 10, Hoene shows:

g. Apparatus for disabling malicious code residing on a customer computer system (Step 178, Figure 3) in a network (Figure 1), the apparatus comprising:

h. means for authenticating the customer (client 20) for the on-line services (Step 152, Figure 3);

i. means for executing, at least in part by activation over the network (Step 158, Figure 3), computer program instructions for performing a scan for the malicious code (McAfee, [0018]), the computer program instructions being directed to detection and disablement of the malicious code (Step 206, Figure 4) in association with providing the on-line services (Step 204, Figure 4) so that the network extends its security perimeter around the customer (the client becomes part of the network by connecting to the server, Figure 1; therefore, the client is considered safe while connected and the virus scan remains active, Steps 180 and 184, Figure 3) while the customer is performing on- line transactions (Step 204, Figure 4).

13. Hoene does not expressly show:

j. association with a financial institution providing on-line financial services to a customer through

k. means for providing the on-line financial services to the customer.

14. However, Antur teaches a secure network (C 1, LL 11-17) with a security perimeter (C 5, LL 47-55) intended for use in financial services from a financial institution (financial services companies, C 1, LL30-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the teachings of Hoene to apply the virus scanning and other control aspects to the financial services network as shown by Antur instead of

the generic network disclosed, in order to counter the risks of endangering information assets (Antur, C 1, LL30-40).

15. As to claim 11, Hoene further shows:

the means for executing the computer program instructions further comprises means for downloading the computer program instructions to the customer computer system (network provided software, [0023]).

16. Claims 3, 6, 7, 9, 12, 15, 18, 19, 21, 24, 27, 28, and 30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hoene and Antur as applied to claims 2, 11, 14, and 23 above, and further in view of Panda ActiveScan.

17. The Hoene/Antur combination discloses as discussed above in regards to claims 2, 11, 14, and 23; and further shows:

the computer program instructions are operable to perform signature-based detection of the malicious code (Step 158, Figure 3).

18. The Hoene/Antur combination does not expressly show:

l. the executing of the computer program instructions is accomplished at least in part through the use of an ActiveX control; and

m. the computer program instructions are operable to perform non-integrity-based unknown malicious code detection.

19. However, Panda ActiveScan shows:

n. the executing of the computer program instructions is accomplished at least in part through the use of an ActiveX control (Release 1, Paragraph 7); and

o. the computer program instructions are operable to perform non-integrity-based unknown malicious code detection (Heuristic scan engine; Release 3, Paragraph 2).

20. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the functions of the anti-virus software in Hoene (McAfee) with the additional functions (n. and o.) of the Panda ActiveScan anti-virus software into one unified software package. These old elements could be combined to perform the same functions as they did separately and one of ordinary skill in the art would have recognized that the result would be predictable.

21. Claims 5, 17, 26, 31, 33, 34, and 36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hoene and Antur as applied to claims 1, 2, 10, 13, 14, 22, and 23 above, and further in view of Applicants' Admitted Prior Art (APA).

22. The Hoene/Antur combination discloses as described above in regards to claims 1, 2, 10, 13, 14, 22, and 23.

23. The Hoene/Antur combination does not expressly show:

p. the computer program instructions are operable to perform integrity checking; and

q. making reference to a database of code that the customer has previously identified as safe.

However, Applicants admit in paragraph 0019 of their specification that integrity checking has been performed by the Norton Anti-Virus software and "making reference to a database of code that the customer has previously identified as safe" is part of integrity checking. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the functions of the anti-virus software in Hoene (McAfee) with the integrity checking of the Norton Anti-Virus software into one unified software package. These old elements could be combined to perform the same functions as they did separately and one of ordinary skill in the art would have recognized that the result would be predictable.

24. Claims 8, 20, 29, 32, and 35 are rejected under 35 U.S.C. §103(a) as being unpatentable over the Hoene/Antur/Panda ActiveScan combination as applied to claims 3, 15, and 24 above, and further in view of APA.

25. The Hoene/Antur/Panda ActiveScan combination discloses as described above in regards to claims 3, 15, and 24.

26. The Hoene/Antur/Panda ActiveScan combination does not expressly show:

r. the computer program instructions are operable to perform integrity checking; and

s. making reference to a database of code that the customer has previously identified as safe.

27. However, Applicants admit in paragraph 0019 of their specification that integrity checking has been performed by the Norton Anti-Virus software and "making reference to a database of code that the customer has previously identified as safe" is part of integrity checking. It would have been obvious to one of ordinary skill in the art at the time of the invention to

combine the functions of the anti-virus software of the combination (McAfee/Panda ActiveScan) with the integrity checking of the Norton Anti-Virus software into one unified software package. These old elements could be combined to perform the same functions as they did separately and one of ordinary skill in the art would have recognized that the result would be predictable.

Claim Interpretations

28. Applicants stated in their specification:

> *"[0019] Integrity checking (called "inoculation" by the commercial Norton TM Anti-Virus product from Symantec Corp.) is a technique in which "snapshots" or "fingerprints" are taken of programs (executable files, boot records) on the computer under the assumption that all these files are in an uninfected state. These fingerprints are typically taken after the computer has been scanned with a scanner that reasonably assures the computer is virus-free. These fingerprints are then saved into a database for later integrity-based scans. During subsequent integrity-based scans of the computer, the antivirus program verifies that each previously fingerprinted program on the computer matches its fingerprint. If a program does not match its fingerprint, then the antivirus program typically uses artificial intelligence to determine if the modification is malicious or merely a valid program update. In some cases, if the scanning software is still unsure, it asks the user to verify whether the new or changed program is legitimate. An integrity checking system can be adapted for use in the context of the invention by making a record of the code the customer has installed in the databases when a customer first access the financial services web site and makes use of the scanning services."*

29. Applicants, in this statement, clearly attribute integrity checking to Symantec Corporation. The Examiner has relied upon this as admitted prior art in the formulation of the art rejections above.

Response to Arguments

30. Applicant's arguments with respect to claims 1-36 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

31. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to JOSHUA MURDOUGH whose telephone number is (571)270-3270. The Examiner can normally be reached on Monday - Thursday, 7:00 a.m. - 5:00 p.m.

32. If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

33. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. M.
Examiner, Art Unit 3621

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621